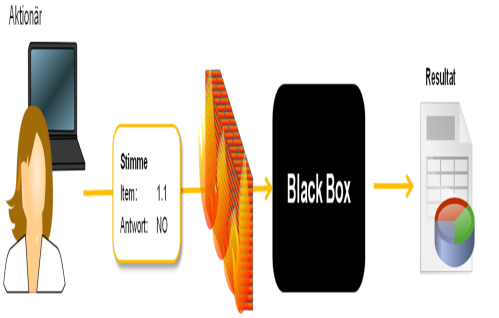
Halm Reusser

Christoph Galliker

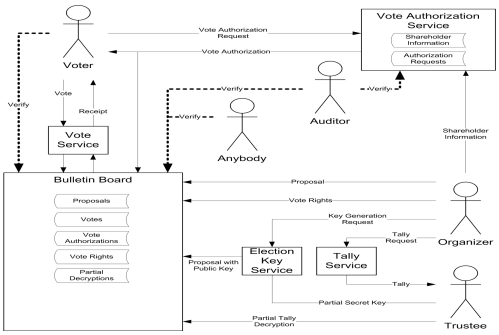
Diplomanden	Halm Reusser, Christoph Galliker
Examinator	Prof. Dr. Andreas Steffen
Experte	Prof. Dr. Eric Dubuis, Berner Fachhochschule, Biel
Master Research Unit	Software and Systems
Projektpartner	UBS, Zürich

Primevote

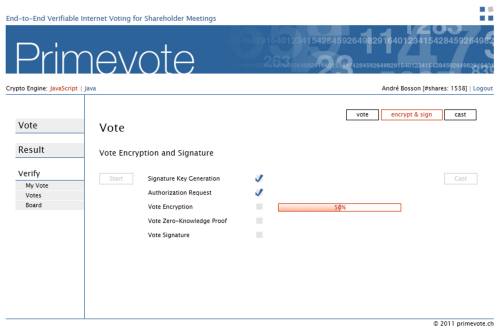
End-zu-End verifizierbares Internetvoting für Generalversammlungen



Blackbox Ansatz ohne Transparenz und Verifizierbarkeit.



Konzept: Akteure und Komponenten.



Abstimmen via Webbrowser: Autorisierung, Verschlüsselung, Zero-Knowledge Proof und digitale Signatur.

Die Shareholder Services von Grossunternehmen möchten ihren Aktionärinnen und Aktionären die Möglichkeit geben, via Internet zu den Traktanden der Generalversammlung abzustimmen oder sogar live von zu Hause daran teilzunehmen. Der Hauptgrund, weshalb diese Möglichkeit heute noch nicht existiert, ist die kritische Beurteilung der Sicherheit.

Diese Arbeit präsentiert ein Konzept, das den Aktionären erlaubt ihre Stimme über das Internet abzugeben. Um die hohen Sicherheitsanforderungen zu erfüllen, werden moderne kryptographische Methoden angewendet. Dadurch können die Aktionäre verifizieren, dass ihre Stimmen wie gewünscht gezählt wurden und das Resultat korrekt ist, ohne dabei den Schutz der Privatsphäre zu verlieren. Anhand dieses Konzeptes wurde Primevote implementiert.

Primevote ist eine funktionsfähige Demoplattform, mit welcher sich Abstimmungen aufsetzen, durchführen und überprüfen lassen. Als Basis wurde das Damgaard- Jurik E- Voting Protokoll verwendet. Die Stimmen der Aktionäre können dabei im verschlüsselten Zustand anhand des Aktienbesitzes gewichtet und zusammengezählt werden. Durch Zero-Knowledge Proofs wird sichergestellt, dass nur gültige Stimmen gezählt werden und die Entschlüsselung des Resultates korrekt ist. Da der Schlüssel zur Entschlüsselung auf mehrere Vertrauenspersonen verteilt ist, wird für die Veröffentlichung des Resultates die Zustimmung von diesen benötigt. Die Verteilung des Schlüssels wird im Protokoll von Damgaard- Jurik durch eine vertrauenswürdige Instanz durchgeführt. Diese wäre aber in der Lage, das Resultat alleine zu entschlüsseln.Um diesen Nachteil zu beseitigen, wurde in Primevote das Protokoll von Nishide und Sakurai integriert. Mit diesem kann der Schlüssel von den Vertrauenspersonen verteilt generiert werden.